The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
5/6/2010

SUBJECT:
Microsoft Windows SMTP Server DNS Spoofing Vulnerabilities

OVERVIEW:
Two new vulnerabilities have been discovered in the Microsoft SMTP (Simple Mail Transfer Protocol) service that could lead to the disclosure of information. Microsoft Windows SMTP service is a component that allows emails to be sent and received. These vulnerabilities could be exploited if an attacker creates a specially crafted query that is designed to exploit these vulnerabilities. This could allow an attacker to redirect network traffic which could lead to the unauthorized disclosure of information.

Please note that both of these vulnerabilities were fixed by the patches referenced in MS10-024, dated April 13, 2010, but were not disclosed in this security bulletin.

SYSTEMS AFFECTED:
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows 2003
- Microsoft Windows 2008
- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: NA

DESCRIPTION:
Two new vulnerabilities have been discovered in the Microsoft Windows SMTP (Simple Mail Transfer Protocol) service. The first vulnerability is caused because the server fails to validate DNS responses. This occurs only if the value of the ID field of a DNS

response received matches the value of the ID field of a corresponding DNS query packet previously sent. The second vulnerability is caused by the server failing to use sufficiently random values for DNS query IDs. It should be noted that the Microsoft Windows SMTP Service performs its own DNS resolution of MX records rather than use the DNS resolver from the operating system.

These vulnerabilities could allow an attacker to redirect network traffic which could lead to the unauthorized disclosure of information via a man-in-the-middle attack.

Please note that both of these vulnerabilities were fixed by the patches referenced in MS10-024 but were not disclosed in Microsoft's security bulletin. These patches only need to be applied to systems running the Microsoft Windows SMTP service such as Windows servers running Internet Information Services (IIS) or Microsoft Exchange Server. Note that Windows XP desktops can also run IIS, and will need to have the appropriate patch applied only if Microsoft Windows SMTP Services is installed.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

REFERENCES:
Core Security Technologies:
http://www.coresecurity.com/content/CORE-2010-0424-windows-smtp-dns-query-id-bugs

Microsoft:
http://www.microsoft.com/technet/security/Bulletin/MS10-024.mspx

Security Focus:
http://www.securityfocus.com/bid/39908
http://www.securityfocus.com/bid/39910

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-1689
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-1690